UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,194	02/12/2002	Klimenty Vainstein	2222.5390003	7090

26111 7590 02/15/2011

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
02/15/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/075,194	VAINSTEIN ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/30/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 11/30/2010 has been entered. Applicant has amended claims 1, 21, 34, 35, 45 and 46. Currently claims 1-46 are pending in this application.

Response to Arguments

Applicant's arguments filed 11/30/2010 have been fully considered but they are not persuasive.

Applicant argues that, "The Examiner argues that the identifier recited in claim 1 is analogous to identifying a corresponding copy of a wrapped key in Langford through the use of a *key identifier* associated with a recipient. (Office Action, p. 8) (emphasis added). However, this is different from "a corresponding *user or group identifier,"* as recited in amended claim 1. In particular, although Langford can use the techniques to send messages to members of a group (see, e.g., Langford, 1:59-62), there is no determination of a "sub-header's correspondence to the user or to the group to which the user belongs *based on a corresponding user or group identifier,"* as recited in claim 1."

Examiner respectfully disagrees and would like to point out that key identifier can be interpreted as a corresponding user or group identifier because Langford at Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by

reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message." Therefore, the key identifier not only identifies the key but also the group or a user as taught by Langford.

Applicant further argues that, "Moreover, the Examiner argues in the "Response to Arguments" section of the Office Action that Richards allegedly supplies the teaching of "access rules applicable to the user or to a group to which the user belongs," as further recited in claim 1. (Office Action, p. 3). However, the Examiner bases this on "[t]he policy component 114 includes elements that define recipient's access rights to the data," and again not to any "user or to the group to which the user belongs based on a corresponding user or group identifier."

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Applicant should note that Langford was relied upon to teach individual encrypted sub-header of the secure item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups, based on the sub-header's correspondence to other users or groups to which the user belongs based on an identifier. The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user

belongs for the secured item. Finally, Richards was used to disclose a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item. Applicant should note that when the teaching of Richards are applied to the header of Langford, a person of ordinary art can readily modify the sub-headers corresponding to multiple groups in Langford to have access rules for each sub-header part.

Applicant further argues that, "In claim 1, the access rules in question are located in the encrypted sub-header, which is itself selected "based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier." Accordingly, it is insufficient to allege that Langford teaches an identifier (which is, as noted, specifically not a user or group identifier), and to further allege that Richards teaches access rules applicable to a user (the message recipient, not identified by a user or group identifier), as this lacks applicability of the access rules based on correspondence to a "user or group identifier."

Examiner would like to point out that the current language of claim 1 recites, "the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item, the sub-header selected, from a group of individually encrypted sub-headers corresponding to other users or groups, based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier". Applicant should note that the selection step is based on the sub-header's correspondence to the user or group

identifier. Claims language does not require "access rules based on correspondence to a "user or group identifier" as argued by the applicant.

Applicant further argues, "As a result, even assuming, arguendo, that Langford teaches selection of a sub-header "based on the sub-header's correspondence to the user or to the group to which the user belongs based on a corresponding user or group identifier" (which is not the case, as the cited key identifier is not the same as a user or group identifier), Richards cannot be used to supply the missing teaching of "the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item," because no mechanism is present in the combination of Langford and Richards to associate access rules as applicable to "the user or to a group to which the user belongs." In claim 1, this is accomplished by the presence of the access rules in the appropriate sub-header associated with a "user or group identifier", but no such mechanism exists in the combination of Langford and Richards. "

As pointed out before, the combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item. Finally, Richards was used to disclose a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item. Applicant should note Richards discloses access rules applicable to the user (Please note that the language "or to a group to which the user belong" is optional) and when the teaching of

Richards are applied to the header of Langford, a person of ordinary art can readily modify the sub-headers corresponding to multiple groups in Langford to have access rules for each sub-header part because Langford discloses encrypted sub-header for different groups. Therefore, the combination of Russell, Langford and Richards discloses "the encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item".

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim(s) 34-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim(s) 34-35 are directed towards a "tangible computer-readable medium" that stores instructions. While specification at paragraph 0156 mentions "computer-readable medium", specification does not define the term. Thus it is unclear whether the term is meant to encompass signals or not. Please note that adding a tangible to the "computer-readable medium" does not exclude the signals because when one goes to the dictionary, tangible is defined as capable of being touched (good) or perceived (bad). A signal can be perceived i.e. sound waves. The broadest, reasonable interpretation of the term is applied and currently the examiner is assuming that "tangible computer-readable medium" encompasses signals. Signals do not fall within

any of the four statutory categories of invention, thus claims 34-35 are not statutory. Examiner suggests amending claims to recite, "non-transitory computer-readable recording medium" to exclude non-statutory mediums such as signals (see, *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under 35 U.S.C. § 101*, Aug. 24, 2009; p. 2 and also Memorandum on Subject Matter Eligibility of Computer Readable Media, Jan 26, 2010).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19, 21-32 and 34-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell et al. (WO 01/77783 A2), hereinafter, "Russell" in view of Langford et al. (US 6,266,420 B1), hereinafter, "Langford". and further in view of Richards et al. (US 2002/0016922 A1), hereinafter, "Richards".

Regarding **Claims 1 and 34**, Russell discloses method and corresponding computer program for providing access management through use of a plurality of server machines associated with different locations (see, Fig. 1), said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location (see, page 24, lines 2-7);

authenticating a user of the first client machine at the first location (see, Page 11, lines 30-31);

authenticating the first client machine (See, Page 25, lines 6-14);

retrieving at the first server machine access rules for the secured item based on the success of said authentication of the user and authenticating of the first client machine (see, Page 25, lines 23-30);

permitting access to the secure item via the first location based on success of said authenticating of the user and authenticating of the first client machine and further based on allowability by the access rules (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13);

permitting access to the secure item via the first server machine based on said permitting access to the secure system via the first location permitting the user to gain access to the secure item from the first location (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13); and

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secured item and the sub-header selected, from a group of individually encrypted sub-headers corresponding to other

user or groups, based on the sub-header's correspondence to other users or groups to the user or to a group to which the user belongs based on an identifier.

Langford discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item (see, Fig. 2, and also Column 3, 53-55, "The group security credentials include at least a public encryption key and a private decryption key" and also Column 2, lines 45-46, "the header will contain the symmetric key wrapped only with the public key of the group), the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups (see, Column 2, lines 52-54, "Note that a single message could be sent to multiple groups simultaneously; in this case, the header contains a wrapped symmetric key for each group"), based on the sub-header's correspondence to other users or groups to which the user belongs based on a corresponding user or group identifier (see, Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place file key of Russell into encrypted sub-headers as taught by Langford because "With such a method and apparatus, group communications are secured and transmitted using security credentials of the group. As

such, the data overhead that accompanies each secured message is substantially reduced in comparison with expanding the recipient list and securing the communication using the security credentials of each of the members." (See, Langford, Column 2, lines 55-60).

The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0068, "The policy component 114 includes elements that define recipient's access rights to the data, such as the rights to "read/write", "save encoded", "save open", "no save", "server keyed", "render 1", "render 2", "Age 1", "Age 2", and "Use", etc.").

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access rules, in the individual encrypted sub-headers of the combination of Russell and Langford, as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 21 and 35**, Russell discloses method and corresponding computer program for providing access management through use of a distributed network of server machines (see, Fig. 1), said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine (see, page 24, lines 2-7);

authenticating a user of the client machine (see, Page 11, lines 30-31);

authenticating the first client machine (See, Page 25, lines 6-14);

upon successfully authenticating the user and authenticating the first client machine, retrieving access rules for the secure item (see, Page 25, lines 23-30);

retrieving access privileges associated with the user (see, Page 25, lines 23-30);

determining whether the user is permitted to gain access to the secure item via the first server machine based on success of said authentication the user and said authenticating the first client machine and further based on allowability by the access privileges and access rules (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13);

permitting access to the secure item via the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is permitted to gain access to the secure item via the first server machine (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13); and

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secured item and the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups, based on the sub-header's correspondence to other users or groups to the user or to a group to which the user belongs based on an identifier.

Langford discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item (see, Fig. 2, and also Column 3, 53-55, "The group security credentials include at least a public encryption key and a private decryption key" and also Column 2, lines 45-46, "the header will contain the symmetric key wrapped only with the public key of the group), the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups (see, Column 2, lines 52-54, "Note that a single message could be sent to multiple groups simultaneously; in this case, the header contains a wrapped symmetric key for each group"), based on the sub-header's correspondence to other users or groups to which the user belongs based on a corresponding user or group identifier (see, Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place file key of Russell into encrypted sub-headers as taught by Langford because "With such a method and apparatus, group communications are secured and transmitted using security credentials of the group. As such, the data overhead that accompanies each secured message is substantially reduced in comparison with expanding the recipient list and securing the communication using the security credentials of each of the members." (See, Langford, Column 2, lines 55-60).

The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0068, "The policy component 114 includes elements that define recipient's access rights to the data, such as the rights to "read/write", "save encoded", "save open", "no save", "server keyed", "render 1", "render 2", "Age 1", "Age 2", and "Use", etc.").

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access rules, in the individual encrypted sub-headers of the combination of Russell and Langford, as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or

stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 2**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses wherein said determining permitting access to the secure system via the first location comprises: obtaining access privileges associated with the user to determine at least one or more permitted locations for the user; and determining whether the user is permitted to gain access to the secure item from the first location based on the permitted locations associated with the user (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 3**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses wherein permission by said permitting access to the secure system via the first location further comprises allowing access to the secure item from the first location via the first client machine and the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 4**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses wherein permission by said permitting access to the secure item via the first server machine further comprises allowing access to the secure item from the first location via the first client machine and

the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claims 5 and 22**, the rejections of claims 1 and 21 are incorporated and the combination of Russell, Langford and Richards further discloses preventing access to the secure item via any of the server machines other than the first server machine based on permitting access to the secure item via the first server machine permitting the user to gain access to the secure item from the first location (see Russell, Page 29, lines 1-4).

Regarding **Claims 6 and 23**, the rejection of claims 1 and 21 are incorporated and the combination of Russell, Langford and Richards further discloses wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first client machine and the first server machine, and wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first client machine and the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via both the first client machine and the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 24**, the rejections of claim 23 is incorporated and the combination of Russell, Langford and Richards further discloses preventing access to the secure item via any of the server machines other than the first server machine when

said determining whether the user is permitted to gain access to the secure item via the first server machine determines that the user is permitted to gain access to the secure item from the first location (see Page 29, lines 1-4).

Regarding **Claim 7**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first server machine, and wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via the first server machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 8**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses wherein said permitting access to the secure system via the first location comprises determining whether the user is permitted to gain access to the secure item via the first client machine, and wherein said permitting access to the secure item via the first server machine operates to permit the user to gain access to the secure item via the first client machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item via the first client machine (see Russell, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13).

Regarding **Claim 9**, the rejection of claim 1 is incorporated and the combination of Russell, Langford and Richards further discloses preventing the user from gaining access to the secure item via any of the server machines other than the first server machine based on said permitting access to the secure system via the first location determining that the user is permitted to gain access to the secure item from the first location (see Page 29, lines 1-4).

Regarding **Claims 10 and 25**, rejections of claims 9 and 24 are incorporated and the combination of Russell, Langford and Richards further discloses

wherein said preventing the user from gaining access to the secure item via any of the server machines other than the first server machine comprises reconfiguring at least one of the server machines that previously permitted the user to gain access to the secure item therethrough (see, Russell, Page 25, line 22- Page 26, line 2).

Regarding **Claims 11 and 26**, the rejections of claims 10 and 25 are incorporated and the combination of Russell, Langford and Richards further discloses said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine (see, Russell, Page 24, lines 14-22).

Regarding **Claim 12**, the rejection of claim 13 is incorporated and the combination of Russell, Langford and Richards further discloses wherein said permitting access to the secure system via the first location comprises: obtaining access privileges associated with the user to determine at least one or more permitted locations for the user (see, Russell, Page 25, lines 11-14); and determining whether the user is permitted

to gain access to the secure item from the first location based on the permitted locations associated with the user (see, Russell, Page 25, lines 11-14).

Regarding **Claims 13 and 27**, rejections of claims 1 and 21 are incorporated and the combination of Russell, Langford and Richards further discloses wherein said permitting access to the secure item via the first server machine comprises reconfiguring the first server machine to permit access by the user to the secure item via the first server machine (see, Russell, Page 24, lines 14-22).

Regarding **Claims 14 and 28**, rejections of claims 13 and 21 are incorporated and the combination of Russell, Langford and Richards further discloses wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file, the secured file having a format that comprises a header including security information as to who and how access to the secure item is permitted (see, Richards, Fig. 4 and Paragraphs 0066-0068); an encrypted data portion including data of the secured file encrypted with a file key according to a predetermined cipher scheme, and wherein the header is attached to the encrypted data portion to generate the secured file (see, Langford, Fig. 1).

Regarding **Claims 15 and 29**, rejections of claims 14 and 28 are incorporated and the combination of Russell, Langford and Richards further discloses wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file the security information in the header of the secured file facilitates the restricted access to the secured file (see, Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claim 16**, the rejection of claim 15 is incorporated and the combination of Russell, Langford and Richards further discloses wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file the security information in the header of the secured file points to or includes the access rules and a file key (see, Langford, Fig. 1 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claims 17 and 30**, rejection of claims 14, and 28 are incorporated and the combination of Russell, Langford and Richards further discloses wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file the security information is encrypted with a user key associated with the user (see, Langford, Fig. 1).

Regarding **Claims 18 and 31**, rejections of claims 14 and 28 are incorporated and the combination of Russell, Langford and Richards further discloses wherein receiving the access request comprises receiving the access request to access the secure item comprising a secured file the security information includes the file key and access rules to the restricted access to the secured file (see, Langford, Fig. 1 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claims 19 and 32**, rejections of claims 18 and 28 are incorporated and the combination of Russell, Langford and Richards further discloses wherein the file key is retrieved to decrypt the encrypted data portion in the secured file based on access privilege of the user being within access permissions by the access rules (see, Langford, Fig. 1 as combined with Richards, Fig. 4 and Paragraphs 0066-0068).

Regarding **Claim 36**, Russell discloses an access control system that restricts access to a secure item (see, Fig. 1), said system comprising:

a central server having a server module that provides overall access control (see, page 16, lines 18-23); and

a plurality of local servers, each of said servers including a local module that provides local access control (see, Page 24, lines 14-22),

wherein the access control, performed by said central server or said local servers, operates to permit or deny access requests to secured items by requestors (see, Page 16, lines 18-23), and

permitted to access the secure item through one or more of said local servers, is only able to access the secure item using only a single one of said local servers or the central server such that the given requestor is only permitted to access the secure item through at most one of said local servers at a time (see, Page 24, 14-22).

Russell discloses controlling access to a secure file. Russell does not explicitly discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item and wherein the individually encrypted sub-header is selected for decryption by the given requestor from a group of one or more additional individually encrypted sub-headers corresponding to other requestors or groups to which the other requestors belong based on correspondence of the individually encrypted sub-header to an identifier for the given requestor or to a group to which the requestor belongs.

Langford discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item (see, Fig. 2, and also Column 3, 53-55, "The group security credentials include at least a public encryption key and a private decryption key" and also Column 2, lines 45-46, "the header will contain the symmetric key wrapped only with the public key of the group), the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups (see, Column 2, lines 52-54, "Note that a single message could be sent to multiple groups simultaneously; in this case, the header contains a wrapped symmetric key for each group"), based on the sub-header's correspondence to other users or groups to which the user belongs based on a corresponding user or group identifier (see, Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place file key of Russell into encrypted sub-headers as taught by Langford because "With such a method and apparatus, group communications are secured and transmitted using security credentials of the group. As such, the data overhead that accompanies each secured message is substantially reduced in comparison with expanding the recipient list and securing the communication

using the security credentials of each of the members." (See, Langford, Column 2, lines 55-60).

The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach the information stored in the individually encrypted sub-header of the secure item comprising access rules applicable to the requestor or to a group to which the requestor belongs.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules applicable to the requestor stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0068, "The policy component 114 includes elements that define recipient's access rights to the data, such as the rights to "read/write", "save encoded", "save open", "no save", "server keyed", "render 1", "render 2", "Age 1", "Age 2", and "Use", etc.").

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access rules, in the individual encrypted sub-headers of the combination of Russell and Langford, as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 37**, the rejection of claim 36 is incorporated and the combination of Russell and Langford further discloses wherein said access control

system couples to an enterprise network to restrict access to the secure item, which comprises a secured file, stored therein (see Russell, Fig. 3).

Regarding **Claim 38**, the rejection of claim 37 is incorporated and the combination of Russell and Langford further discloses wherein the access requests are at least primarily processed in a distributed manner by said local servers (see, Russell, Page 24, lines 14-22).

Regarding **Claim 39**, the rejection of claim 38 is incorporated and the combination of Russell and Langford further discloses wherein the requestors gain access to the secured files without having to access said central server based on processing of the access requests by said local servers (see, Russell, Page 24, lines 14-22).

Regarding **Claim 40**, the rejection of claim 37 is incorporated and the combination of Russell and Langford further discloses wherein the local module is a copy of the server module so any of the local modules can operate independent operate independently of said central server and other of said local servers (see, Page 23, lines 19-22).

Regarding **Claim 41**, the rejection of claim 37 is incorporated and the combination of Russell and Langford further discloses wherein the local module is a subset of the server module (see, Russell, Page 18, lines 15-17).

Regarding **Claim 42**, the rejection of claim 42 is incorporated and the combination of Russell and Langford further discloses wherein access permissions for said local servers is dynamically configured to pass a requestor from one of said local

servers to another of said local servers, thereby enabling access control to be performed by the another of said local servers such as a change of the location of the requestor (see, Page 20, lines 16-31).

Regarding **Claim 43**, the rejection of claim 37 is incorporated and the combination of Russell and Langford further discloses wherein the secured files are secured by encryption of the secure item (see, Page 9, lines 6-7).

Regarding **Claim 44**, the rejection of claim 37 is incorporated and the combination of Russell and Langford further discloses wherein the secure item are secured by encryption (see, page 9, lines 6-7).

Regarding **Claim 45**, Russell discloses method for providing access management through use of a plurality of server machines associated with different locations (see, Fig. 1), said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine at a first location(see, page 24, lines 2-7);

authenticating a user of the first client machine (see, Page 11, lines 30-31);

authenticating the first client machine (See, Page 25, lines 6-14);

retrieving at the first server machine, based on the success of said authentication of the user and authenticating of the first client machine access privileges associated with the user (see, page 25, lines 23-30);

permitting access to the secure item via the first location based on success of said authenticating of the user and authenticating of the first client machine and further based on allowability by the access rules (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13);

preventing access to the secure item via the first server machine based on said permitting access to the secure system via the first location not permitting the user to gain access to the secure item from the first location (see Page 26, lines 7-9).

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secured item and the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups, based on the sub-header's correspondence to other users or groups to the user or to a group to which the user belongs based on an identifier.

Langford discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item (see, Fig. 2, and also Column 3, 53-55, "The group security credentials include at least a public encryption key and a private decryption key" and also Column 2, lines 45-46, "the header will contain the symmetric key wrapped only with the public key of the group), the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups (see, Column 2, lines 52-54, "Note that a single message could be sent to multiple groups simultaneously; in this case, the header contains a wrapped symmetric key for each group"), based on the sub-header's correspondence to other

users or groups to which the user belongs based on a corresponding user or group identifier (see, Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place file key of Russell into encrypted sub-headers as taught by Langford because "With such a method and apparatus, group communications are secured and transmitted using security credentials of the group. As such, the data overhead that accompanies each secured message is substantially reduced in comparison with expanding the recipient list and securing the communication using the security credentials of each of the members." (See, Langford, Column 2, lines 55-60).

The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0068, "The policy

component 114 includes elements that define recipient's access rights to the data, such as the rights to "read/write", "save encoded", "save open", "no save", "server keyed", "render 1", "render 2", "Age 1", "Age 2", and "Use", etc.").

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access rules, in the individual encrypted sub-headers of the combination of Russell and Langford, as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Regarding **Claim 46**, Russell discloses method for providing access management through use of a distributed network of server machines (see, Fig. 1), said method comprising:

receiving, at a first server machine of the plurality of server machines, an access request to access a secure item from a first client machine (see, page 24, lines 2-7);

authenticating a user of the first client machine (see, Page 11, lines 30-31);

authenticating the first client machine (See, Page 25, lines 6-14);

upon successfully authenticating the user and authenticating the first client machine, retrieving at the first server machine access privileges associated with the user (see, page 25, lines 23-30);

determining whether the user is permitted to gain access to the secure item via the first server machine based on success of said authenticating the user and said authenticating the first client machine, and further based on allowability by the access privileges and access rules (see, page 11, lines 30-31, Page 25, lines 6-14 and Page 26, lines 3-13); and

preventing access to the secure item via the first server machine based on said determining whether the user is permitted to gain access to the secure item via the first server machine determining that the user is not permitted to gain access to the secure item via the first server machine (see Page 26, lines 7-9).

Russell discloses encrypting secure content to be delivered however, Russell does not explicitly teach retrieving at the first server machine a user key permitting access to an individually encrypted sub-header of the secured item and the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups, based on the sub-header's correspondence to other users or groups to the user or to a group to which the user belongs based on an identifier.

Langford discloses retrieving at the first server machine, a user key permitting access to an individual encrypted sub-header of the secure item (see, Fig. 2, and also Column 3, 53-55, "The group security credentials include at least a public encryption key and a private decryption key" and also Column 2, lines 45-46, "the header will contain the symmetric key wrapped only with the public key of the group), the sub-header selected, from a group of individually encrypted sub-headers corresponding to other user or groups (see, Column 2, lines 52-54, "Note that a single message could be

sent to multiple groups simultaneously; in this case, the header contains a wrapped symmetric key for each group"), based on the sub-header's correspondence to other users or groups to which the user belongs based on a corresponding user or group identifier (see, Column 4 lines 7-13 clearly recites, "The process then proceeds to step 44 where the member of the group determines whether the secured group communication is a group communication for a particular group. Such a determination is made by reviewing the **key identifier** in the header of the message, if the identifier identifies the group, it is a group message, if it identifies the party, it is an individual message.")

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place file key of Russell into encrypted sub-headers as taught by Langford because "With such a method and apparatus, group communications are secured and transmitted using security credentials of the group. As such, the data overhead that accompanies each secured message is substantially reduced in comparison with expanding the recipient list and securing the communication using the security credentials of each of the members." (See, Langford, Column 2, lines 55-60).

The combination of Russell and Langford discloses individually encrypted sub-headers but does not explicitly teach that the individually encrypted sub-header including access rules applicable to the user or to a group to which the user belongs for the secured item.

However, Richards discloses a system where a given requester is permitted to access a secure item based on access rules applicable to the user stored in an encrypted header of a secure item (see, Fig. 4 and Paragraphs 0068, "The policy component 114 includes elements that define recipient's access rights to the data, such as the rights to "read/write", "save encoded", "save open", "no save", "server keyed", "render 1", "render 2", "Age 1", "Age 2", and "Use", etc.").

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to place access rules, in the individual encrypted sub-headers of the combination of Russell and Langford, as taught by Richards because "all encoded header data, database, and any other data are encoded as a single data file or stream being singular in type, the data may be checked by the application before opening via the various embedded hash elements. Accordingly, the security and integrity of the data is further maintained, firewall requirements are simplified, and the potential of firewall penetration is reduced" (see, Paragraph 0073).

Claims 20 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russell in view of Langford and Richards and further in view of Brown et al. (US 2003/0050919 A1), hereinafter "Brown".

Regarding **Claims 20 and 33**, rejections of claims 18 and 31 are incorporated and the combination of Russell, Langford and Richards further discloses receiving the access request comprises receiving the access request to access the secure item

comprising a secured file with the access rule but does not explicitly disclose access rules expressed in a markup language.

However, Brown discloses access rules expressed in a markup language (see, Fig. 5A and Paragraph 0052).

Therefore, it would have been obvious at the time invention was made to a person of ordinary skill in the art to express the access rules of the combined system of Russell, Langford and Richards in a markup language as taught by Brown because XML is a text-based and platform independent markup language, as a result distributor server would be able to enforce and distribute the content with policies to all client having any type of operating system platform.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F 9:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435

/Nirav B. Patel/

Primary Examiner, Art Unit 2435